FEDERAL GOVERNMENT MODEL PERFORMANCE

A "LEGAL FOUNDATIONS" STUDY

Report 11 of 12

Report to the
President's Commission
on Critical Infrastructure Protection
1997

This report was submitted to the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. This report represents the opinions and conclusions solely of its developers.

Contents

Acknowledgments

The *Legal Foundations* series of reports of the President's Commission on Critical Infrastructure Protection (PCCIP) resulted from the concerted efforts and hard work of several individuals. The Commission gratefully acknowledges Commissioner Stevan D. Mitchell and Assistant General Counsel Elizabeth A. Banker for their leadership and important contributions in developing the *Legal Foundations* series of reports. Their research, writing and analytical contributions were essential to the success of the effort.

The Commission also acknowledges Lee M. Zeichner, Esq. of LegalNet Works Incorporated and his staff, for conceptualizing and maintaining the legal issues database and for providing tireless research support. Finally, the Commission acknowledges the contributions of Senior Consultant Paul Byron Pattak for his deft editing of this compilation.

Preface

Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) and tasked it with assessing the vulnerabilities of, and threats to, eight named critical infrastructures and developing a national strategy for protecting those infrastructures from physical and cyber threats. The Executive Order also required that the PCCIP consider the legal and policy issues raised by efforts to protect the critical infrastructures and propose statutory and regulatory changes necessary to effect any subsequent PCCIP recommendations.

To respond to the legal challenges posed by efforts to protect critical infrastructures, the PCCIP undertook a variety of activities to formulate options and to facilitate eventual implementation of PCCIP recommendations by the Federal government and the private sector. The PCCIP recognized that the process of infrastructure assurance would require cultural and legal change over time. Thus, these activities were undertaken with the expectation that many would continue past the life of the PCCIP itself.

The *Legal Foundations* series of reports attempts to identify and describe many of the legal issues associated with the process of infrastructure assurance. The reports were used by the PCCIP to inform its deliberations. The series consists of 12 reports:

1. *Legal Foundations: Studies and Conclusions*
2. *The Federal Legal Landscape*
3. *The Regulatory Landscape*
4. *Legal Authorities Database*
5. *Infrastructure Protection Solutions Catalog*
6. *Major Federal Legislation*
7. *Adequacy of Criminal Law and Procedure (Cyber)*
8. *Adequacy of Criminal Law and Procedure (Physical)*
9. *Privacy and the Employer-Employee Relationship*
10. *Legal Impediments to Information Sharing*
11. *Federal Government Model Performance*
12. *Approaches to Cyber Intrusion Response*

and two special studies:

- *Information Sharing Models*
- *Private Intrusion Response*

Legal Foundations: Studies and Conclusions is the overall summary report. It describes the other reports, the methodologies used by the researchers to prepare them, and summarizes the

possible approaches and conclusions that were presented to the PCCIP for its consideration. The series has been sequenced to allow interested readers to study in detail a specific area of interest. However, to fully appreciate the scope of the topics studied and their potential interaction, a review of the entire series is recommended.

Part One

Introduction

Issue

What are some of the methods available to the Federal government by which it can unilaterally change its own behavior in order to encourage the private sector, state or local governments to act consistently with infrastructure assurance objectives?[1]

Research Findings

- Performance programs and practices are currently being pursued by the Federal and state governments.

- Performance programs and practices are cost-effective, unilateral actions designed to improve government performance directly and to influence private sector behavior indirectly.

- A current trend in government is the movement toward outcome-based performance management, similar to business practices common in industry. Requiring the development and monitoring of performance measures to track progress in achieving goals allows the government to better meet policy objectives.

[1] Note on Methodology: SRA International performed research to identify successful government programs and best practices employed by these programs. These techniques and methods were then evaluated to determine their suitability for accomplishing infrastructure assurance objectives. The research process consisted of a literature search including searches of relevant Internet web sites such as those maintained by the National Performance Review (NPR) and National Academy of Public Administration (NAPA), and telephone interviews of government experts including individuals within the Office of Management and Budget (OMB) and the General Accounting Office (GAO). Summaries of model performance programs and a contact list containing the names and phone numbers of government experts contacted are available for review.

- While the government may not be able to directly require certain features through its procurement process because of the recent move to off-the-shelf products, it may nonetheless influence the marketplace by incorporating policy objectives in choosing among currently available products.

- Use of best practices is commonplace in the private sector. A clearinghouse for best practices within the government could draw on private sector expertise in order to improve government performance.

- Performance programs and practices are relatively inexpensive to implement and do not require reorganization of the government or the creation of a new government organization. Further study of performance-based options, however, may require a follow-on effort.

Assumptions

- The current trend towards use of performance-based programs within the Federal and state governments are likely to continue to grow and expand.

- Infrastructure assurance objectives can be achieved through performance-based methods.

Background: "Performance-Based" Categories

A number of performance-based practices common in industry and adapted by the government, were identified that have been successfully employed by government programs to achieve policy objectives. Some of the practices such as business process reengineering do not appear immediately applicable to infrastructure assurance, and others involve a level of government intrusion in the private sector that may prove unpopular. Figure 1 summarizes the practices and

concepts determined to be potentially applicable for infrastructure assurance. (As indicated in Figure 1, not all of the practices are applicable to each of the critical infrastructure groups).

Practices & Possible Applications	Telecom	Electrical Power	Gas & Oil	Banking & Finance	Transport	Water Supply	Emergncy Services	Govmnt Services
1. Performance Measurement								
a. Infrastructure Report Card	X	X	X	X	X	X	X	X
b. Publication of Infrastructure Reliability Data	X	X	?	?	X	?	?	?
c. Use ITMRA/GPRA to Increase Federal IT Security	X							
d. High Risk Report for Infrastructure Assurance	X	X	X	X	X	X	X	X
2. Certification of Technologies								
a. Certification of Products Meeting Security Standards	X	?	?	?	?	?		
3. Procurement								
a. Infra. Assurance as Criterion for Fed Procurements	X							
4. Identification & Dissemination of Best Practices								
a. Clearinghouse for Best Practices in IT Security	X							X

Figure 1: Current Government Practices and Possible Applications)

Performance Measurement

Perhaps the most significant trend in government is the movement to outcome-based performance management. With the passage of legislation such as the Government Performance and Results Act (GPRA)[2] and the Information Technology Management Reform Act (ITMRA),[3] all agencies are accountable for achieving strategic goals. At the heart of this movement is performance measurement: the development and monitoring of performance measures to track progress in achieving strategic goals.[4] The GPRA, for example, requires Federal agencies to perform strategic planning and performance management. Specifically, it requires them to (1) define their mission, (2) establish strategic goals linked to the mission, and (3) develop and employ performance measures to track progress in achieving their strategic goals. When the system is fully in place, agencies, in their budget submissions, will have to forecast how funding for each of their programs will lead to specific improvements in the performance measures by fiscal year. In other words, they'll have to show OMB and Congress what is to be expected in return for funding their programs. Each year, agencies will also have to report to OMB and

[2] Pub. L. No. 103-62 (1993).
[3] Pub. L. No. 104-106 (1996).
[4] The Government Accounting Office stressed the importance of performance measurement in its executive guide to *Effectively Implementing the Government Performance and Results Act*, stating,

> "The second key step that successful results-oriented organizations studied take -- after defining their missions and desired outcomes -- is to measure their performance. Measuring performance allows these organizations to track the progress they are making toward their goals and gives managers crucial information on which to base their organizational and management decisions. Leading organizations recognize, as well, that performance measures can create powerful incentives to influence organizational and individual behavior."

Congress whether the prior year's goals in terms of the performance measures were actually achieved and, if not, why. In this way, GPRA will make agencies accountable for achieving strategic goals and allow OMB and Congress to allocate funding based on past and expected performance.

The ITMRA operates in a similar manner, but only in the limited area of information technology. The Act requires that OMB review agency budget proposals and performance measurements for, among other things, adequate information security. The Chief Information Officer (CIO) for each agency is responsible for establishing performance measurements for information technology used by or acquired by his or her agency. The performance measures must evaluate how well the information technology supports agency programs. However, information security is not required to be one of these performance measures (even though it is included in the OMB review process). The ITMRA also links the performance measures to the government procurement process.[5]

This practice of performance measurement is also being successfully applied by state governments. The State of Oregon was recognized by the National Performance Review and Harvard's Kennedy School of Government for its *Oregon Benchmarks* initiative in which it established a number of performance measures, or benchmarks, linked to the state's strategic goals. The objective of the *Oregon Benchmarks* program was to translate the state's strategic goals into measurable objectives and create a report card for measuring progress in achieving the goals. The benchmarks have succeeded in providing a clear framework for engaging people both inside and outside the government in the pursuit of well-defined objectives. They are being used by the Oregon Legislature to develop and evaluate legislative proposals and have also helped to foster cooperation among government agencies and between the public and private sectors.

There are a number of possible applications of performance measurement to infrastructure assurance, and this practice appears to be applicable to all of the infrastructure areas. Following the Oregon example, an agency such as the National Security Council or the Federal Emergency Management Agency could be tasked to coordinate the development and annual preparation of an infrastructure assurance report card. The Federal agencies responsible for oversight of the various critical infrastructures would be required to develop the performance measures to be incorporated in the report card and provide the data as needed to the organization responsible for coordinating the preparation of the report. These agencies may already be capturing much of the data necessary to construct such a report card.

By developing an infrastructure assurance report card, the Federal government would be better able to communicate the status of infrastructure assurance, establish infrastructure assurance goals, and identify areas of high risk on which to focus its efforts and resources. Once valid performance data for infrastructure assurance have been collected, new strategies for improving infrastructure assurance may become apparent. For example, it might be possible to induce private sector owners of the infrastructures to improve assurance by publishing detailed company-specific data for various infrastructure assurance performance measures. As examples

[5] *See* discussion *infra* p. A-5, Procurement.

of this practice, the National Highway Traffic Safety Administration publishes comparative crash safety ratings for each car model, and the Department of Transportation publishes comparative airline on-time statistics. This approach is seen as a form of regulatory oversight.

An alternative to the development of an infrastructure assurance report card with performance measures for all of the infrastructure areas would be to apply performance measurement selectively within the existing GPRA framework. Under this application of performance measurement, infrastructure assurance would be made a strategic goal of the agencies with relationships to those infrastructure areas in which the threat or risk is significant. These agencies would then be required to develop specific infrastructure assurance goals and performance measures to be reported as part of their annual GPRA submissions to OMB.

The development of appropriate performance measures is a difficult task under any circumstances and one that takes time. In addition, there may be some unique problems in applying this practice to infrastructure assurance, particularly in the IT infrastructure area. One difficulty in collecting performance data for infrastructure assurance would be that incidents tend to be discrete events that one tries to prevent and react to rather than a continual activity that generates a stream of performance data. In some cases, such as information system incursions, incidents may occur without the knowledge of those operating the infrastructure. Another problem is that infrastructure owners in the private sector may be unwilling to release data for their infrastructures for fear of exposing themselves to attack. Nevertheless, it should be possible to overcome these measurement problems. For example, the Federal Aviation Administration has successfully tracked data for airline incidents for years. With regard to the problem of unobserved incidents, it may be possible to develop measures of incident prevention such as the percentage of agencies or Federal systems in compliance with IT security standards developed by the National Institute of Standards and Technology (NIST), OMB, or another agency. It might also be possible to conduct surveys of key IT infrastructure owners within the private sector to determine the percentage whose systems meet these security standards. At a minimum, the Federal government could produce an annual “high risk” report, such as those produced by the GAO and the National Transportation Safety Board, highlighting the major assurance risk areas and recent trends within the various infrastructure areas.

Certification Programs

Two model programs within the environmental area were identified involving certifications. In both of the programs it appears that government was able to accelerate the market’s adoption of technologies that support policy objectives through certification of technologies or products that meet certain standards. In 1992 the EPA initiated the Energy STAR program which is designed to reduce air pollution by encouraging the development of energy-efficient office equipment. Under this program the EPA developed energy efficiency standards for office equipment. The program allows manufacturers who choose to participate in the program to affix the Energy

STAR logo on equipment that meet these standards. EPA performs spot checks to determine that equipment displaying the Energy STAR logo does indeed meet the standards. According to the EPA, the Energy STAR program with its certification component has helped to promote the awareness of the availability of energy-saving technologies and accelerate industry's rollout of energy-efficient office equipment.

Based on the early success of the program, the White House issued Executive Order 12845[6] in 1993 directing all Federal agencies to purchase only computers, monitors, and printers that meet the EPA Energy STAR requirements. EPA has since expanded the Energy STAR program to other energy-consuming products such as light fixtures and heating, ventilation, and air conditioning units.

The California Environmental Protection Agency initiated an environmental technology certification program similar to the Energy STAR program in 1993. Unlike the Energy STAR program, however, the California EPA tests each of the products for which certification applications have been submitted to determine that they are effective in preventing or cleaning up pollution. The California program has certified about four dozen technologies and was a 1996 winner of the Innovations in American Government award.

In the standards area, the implementing body will have to carefully distinguish between performance standards and specific technical standards and consider the degree of resistance that each will receive from private industry. Generally, the private sector is less resistant to performance standards than specific standards. This practice of certifying effective technologies would appear to be applicable to at least the telecommunications infrastructure area and perhaps all of the infrastructure areas.

Procurement[7]

With the passage of the Federal Acquisition Streamlining Act of 1994 (FASA)[8] and the Federal Acquisition Reform Act of 1995 (FARA),[9] the Federal government is moving away from the practice of placing specific requirements on contractors and vendors. In fact, the simplified acquisition procedures for goods and services below $100,000 encourages government to purchase standard commercial products whenever possible. FASA and FARA instead encourage the government to use its old standards and requirements to choose the best commercially available product to meet the government's needs.

---

6 Executive Order No. 12845, *Requiring Agencies to Purchase Energy Efficient Computer Equipment* (April 21, 1993).

7 *See also* Appendix A, Summary of Procurement Trends and Legislation.

8 Pub. L. No. 103-355 (1994).

9 Pub. L. No. 104-106 (1995).

Furthermore, the Federal government probably does not have the market clout to directly and significantly influence the products developed by private sector firms through its purchasing decisions. For example, data obtained from GSA and the Information Technology Industry Council (ITI) indicate that the Federal government accounts for only 1.5 to 3.5 percent of worldwide information technology purchases, and this percentage is expected to decrease in the future. However, the Federal government is still a large customer and can lead by example within the IT industry by incorporating information security considerations in its procurement practices. Moreover, the provision of vital government services represents a critical infrastructure area and government is increasingly dependent on information technology to provide services.

Therefore, it makes sense for the Federal government to use security as a criteria for its IT purchases if the threat of incursion is serious enough. This does not mean that the Federal government should include security-enhancing design specifications in its acquisitions; rather it should consider security provisions when choosing among currently available IT products.

There are a number of ways that this practice could be implemented. One indirect approach would be for the OMB, GAO, or CIO Council to develop guidelines for incorporating security safeguards in IT acquisitions. Among the more direct approaches, OMB could require agencies to include computer security plans in their budget submissions for proposed IT acquisition programs. OMB would then review these security plans as part of the budget process. The Administration should be very cautious, however, in recommending the use of the procurement process to achieve IT security goals. It must also be careful not to recommend an approach that will delay procurements or increase the cost and reduce the effectiveness of future government systems by placing unnecessary constraints on IT acquisitions. However, with the current re-competition of the FTS2000 contract, which provides telecommunications services for the majority of the Federal government, and many Federal agencies planning new IT applications to support their missions, there may be a significant opportunity to incorporate security safeguards within the government's IT infrastructure through the procurement process.

Identification and Dissemination of Best Practices

In recent years the practice of benchmarking and searching for best practices has become commonplace within private industry. The practice has also gained acceptance within the Federal government. For example, the ITMRA requires OMB to encourage the use of best practices in the acquisition of information technology.

Consistent with this concept, an agency, or agencies, be designated to serve as a clearinghouse within the Federal government for infrastructure assurance practices. This clearinghouse function should be performed in close conjunction with the private sector in order to leverage the expertise of private industry.

Part Two

Options For Model Performance

The options presented are based on performance-based categories discussed more fully in the section above. The option categories and the options themselves are not mutually exclusive and in many cases will be most effective when combined with other model performance programs.

Performance Measurement

The development of an appropriate set of infrastructure performance goals and measures appears to be an essential prerequisite for any infrastructure assurance program. Without them, it will be difficult to define the objectives and scope of the governments' infrastructure assurance efforts and virtually impossible to determine whether or not progress is being made. Without quantitative performance measures it will also be difficult to effectively communicate the need for increased infrastructure assurance. In fact, in the current GPRA environment, Congress and OMB will require the development of performance goals and measures for any infrastructure assurance program before it provides funding.

Develop And Prepare Annual High-Risk Report For Infrastructure Assurance

Under this option, a particular government organization or agency would coordinate the development and preparation of a report listing the areas within the nation's infrastructure facing the highest risk to cyber and physical threats. For each high-risk area, the report would describe the nature of the threats to the infrastructure and the risks they present. The preparation of this report would require the cooperation of the government agencies responsible for the various infrastructure areas. It might also be necessary to obtain information from private sector organizations and state and local governments to prepare the report. However, since the report would mainly be qualitative in nature, most of the necessary information would probably be available within the government.

- **Pro:** This approach would increase awareness of high-risk infrastructure areas and provide some indication of degree to which high risk areas were being addressed. It would also help to focus infrastructure improvement efforts. This approach could be developed very quickly and would be very inexpensive to prepare on a regular basis.

- **Con:** This approach would tend to result in a subjective listing. It runs the risk of not providing much substantiation for high-risk areas and would not be very useful for determining or communicating progress in improving infrastructure assurance.

"Infrastructure Assurance" Is Designated As A Strategic Goal For Federal Agencies To Be Addressed Within GPRA And ITMRA Frameworks

Under this option, infrastructure assurance is either appended to the mission or, more likely, assigned as a strategic goal by executive order to each of the Federal agencies with links to industries with critical infrastructures. If there are only a few high-risk infrastructures it may be necessary to assign infrastructure assurance as goal to only a few agencies. The effectiveness of this option would probably depend on the degree of specificity with which the Federal government could define the infrastructures to be protected, the nature of the threats, and its desired infrastructure assurance goals. Under GPRA, each of the agencies receiving the assignment would be required to develop specific strategic goals for infrastructure assurance, strategies for achieving the goals, and outcome-based performance measures to track progress in achieving the goals. OMB could then prepare an annual, consolidated status report on infrastructure assurance based on the performance data and narrative information provided by agencies in their annual budget submissions and performance reports. Revisions to the ITMRA to include security in information technology management considerations would also link infrastructure assurance objectives to the developing government management process.

- **Pro:** This approach would institutionalize infrastructure assurance as a mission of the Federal government by directly linking it to the budget process. It would also force agencies assigned the mission of protecting infrastructures to devise outcome-based infrastructure assurance strategies and programs.

- **Con:** This approach would place an additional performance reporting requirement on government agencies at a time when they are just beginning to implement performance management. It might fail to develop coordinated efforts among Federal agencies, and

it could encourage development of unnecessarily costly infrastructure assurance programs.

Establish An Interagency Task Force To Investigate The Feasibility Of Developing An Infrastructure Assurance "Report Card"

The development of a concise, quantitative, annual "report card" for infrastructure assurance (similar in format to that developed by the State of Oregon), would provide the Federal government with a powerful tool for raising awareness of the need for infrastructure assurance and communicating the status of infrastructure assurance. It would also help policy makers establish infrastructure assurance goals and identify areas of high risk on which to focus its efforts and resources. Under this option, the Administration could recommend the formation of a follow-on task force to determine whether it is possible to develop such a summary report for infrastructure assurance and, if so, which government organizations should be responsible for preparing the report and what data and resources might be needed.

- **Pro:** This approach recognizes the difficulty in developing appropriate performance measures. The report would be a powerful tool for communicating infrastructure assurance goals and for tracking progress in achieving them. The report would also help to focus and justify subsequent government infrastructure assurance initiatives.

- **Con:** A follow-on study does not represent immediate action to protect critical infrastructures. The report would not make any government agency accountable for achieving infrastructure assurance goals.

Establish An Interagency Task Force To Develop An Infrastructure Assurance Report Card

In the alternative, an interagency task force could be formed to develop the report, or a particular agency could be assigned the responsibility of coordinating development with the assistance of other agencies as needed. It probably would not be necessary to include members of the private sector directly on the report development team, but this might be a good strategy for a number of reasons. If a considerable amount of the data required for the report will have to be obtained from the private sector or state and local governments, involvement of these stakeholders in the development of the report may make them more willing to provide the necessary data.

Involvement of external stakeholders in the development of the report would also help to ensure that performance measures included in the report are valid. Finally, the involvement of external stakeholders would help in gaining widespread buy-in of the results presented in the report.

- **Pro:** This report would be powerful tool for communicating infrastructure assurance goals and for tracking progress in achieving them. It would also help to focus and justify subsequent government infrastructure assurance initiatives.

- **Con:** The report would probably not be capable of making any government agency accountable for achieving infrastructure assurance goals.

Publication of Infrastructure Reliability Data

This approach potentially represents an inexpensive strategy that may be quite effective for certain infrastructure areas.

Investigate Applicability Of Publishing Infrastructure Reliability Data

A study could be performed to determine where among the infrastructure areas this practice might be applicable and effective, and the extent to which it can be accomplished by existing government structures within the framework of existing data collection efforts. This course may also be a logical outgrowth of an effort to develop an infrastructure assurance report card as described above.

- **Pro:** This option would allow time to develop valid measures of infrastructure reliability and security. It would also provide time to gauge stakeholder reaction to the concept.

- **Con:** A general recommendation is less likely to be implemented and a recommendation to perform a follow-on study implies that more time will pass before specific action is taken.

Conduct A Pilot Study On The Feasibility Of Publishing Comparative Telecommunications Or Electric Utility Reliability Data

The Administration could direct the Federal Communications Commission (FCC), the Network Reliability and Interoperability Council (NRIC), the Federal Energy Regulatory Commission (FERC), or the North American Electric Reliability Council (NERC) to perform a pilot study of the feasibility of publishing comparative data of the service reliability among either the telecommunications or electric service providers. The study would also address the degree to which reliability assurance might also achieve desirable infrastructure assurance objectives. If the results of the pilot study indicate that the practice is likely to effective in promoting infrastructure assurance objectives among telecommunications or electric service providers, then the government can implement the practice for the telecommunications or electric service industry and investigate the feasibility of applying the practice to others.

- **Pro:** This option appears to be good test of this practice, since telecommunications and electric industries are being deregulated to spur competition, and consumers are likely to be concerned about the continuing reliability of these services. A pilot study conducted by an existing government or government-sponsored industry council would be relatively inexpensive and likely to be more cost-effective than broad study of applicability of concept across all critical infrastructure areas performed by new interagency task force. A more focused study by organizations designed promote infrastructure reliability and with access to reliability data may lead to a faster implementation of the concept. Since NRIC and NERC include significant industry representation, having either of these organizations perform a pilot study would provide immediate stakeholder reaction to the concept of publishing comparative reliability data and help gain buy-in for the concept.

- **Con:** Increased infrastructure reliability may not necessarily translate to increased infrastructure protection or security. Current reliability may be so high in these industries that consumers base their purchasing decisions on factors other than reliability, such as price. Given the use of shared networks and other facilities in these industries, individual providers may not be able to adequately influence reliability figures.

Begin Publication Of Specific Infrastructure Reliability Data

Under this option, the government would begin publishing detailed data comparing infrastructure reliability and security among private sector owners within particular industries. In order for this to be effective, it would have to be specified which agencies should publish what types of reliability and security data.

- **Pro:** This option would result in highly visible actions in the near future that would help to promote awareness of the issue of infrastructure assurance.

- **Con:** Without knowing what kind of data are available for each of the infrastructure areas it may be premature to recommend publishing comparative data. There is also the risk that by rushing to implement this practice the government could publish data that present an inaccurate comparison of the infrastructure reliability or security among the various private sector owners. This might expose the government to some kind of legal liability or at least poison relations between the government and the private sector organizations it needs to partner with to enhance infrastructure assurance. Rushing to publication might also result in measures that service providers can "game," again leading to invalid comparisons.

Identification And Dissemination Of Best Practices

Recognition of IT security problem is increasing as is the number of products and procedures designed to enhance IT security. Failure to establish a government clearinghouse for best practices in IT security will delay the adoption of such practices within the Federal government and, perhaps, the private sector. This approach also ignores the potentially significant need in other infrastructure areas, where assurance needs are less well recognized, to identify and disseminate best practices in infrastructure assurance. Finally, the identification of standards underlying best practices appears to be a prerequisite for employing any certification practice.

NIST, Commerce, NSA Or Some Other Agency Be Assigned To Serve As Clearinghouse For Best Practices In IT Security

Under this option, the tasked agency would work with private industry to determine the best practices in IT security including those technologies, products, and procedures that offer the best mitigation and assurance from cyber threats as well as those that provide the best recovery capability from incursions. This expands the current requirement that government CIO's collect and share best practices. The agency would be expected to maintain and disseminate information concerning these best practices to appropriate public or private organizations upon request. These best practices could form the guidelines to be used for auditing the security of Federal information systems. They might also become the basis for establishing security standards for IT products and services that can inform a certification process.

- **Pro:** This option is consistent with the direction of recent legislation. NIST appears to already have a substantial knowledge of IT security and in, FedCIRC, is already disseminating information to other government agencies. This would also test the concept of a Federal clearinghouse for best practices in infrastructure assurance before attempting to expand the concept to other infrastructure areas.

- **Con:** There may already be, or soon be, a private sector organization that government and private sector organizations can look to for guidance on best practices and products in IT security. This approach ignores potentially significant need in other infrastructure areas to identify and disseminate best practices in infrastructure assurance.

NIST, Commerce, NSA Or Some Other Agency Be Assigned To Serve As Clearinghouse For Best Practices In IT Security And The Federal Government Would Investigate The Feasibility/Advisability Of Establishing Clearinghouses For Infrastructure Assurance In Other Infrastructure Areas

Under this option, a specific approach to establish NIST, Commerce, NSA or another government agency as a clearinghouse for best practices in IT security within the Federal government would be combined with a more general recommendation to study the applicability of the clearinghouse concept to the other critical infrastructure areas.

- **Pro:** This approach would address the immediate need in the IT infrastructure area as well as that of the other critical infrastructure areas.

- **Con:** In order to ensure that the study of the applicability of the clearinghouse concept to other, non-IT infrastructure areas is performed, a follow-on task force would have to be formed or a specific agency would have to be assigned the task of performing the study. This assignment would compete with and might dilute the efforts of any follow-on task force assembled to implement infrastructure assurance efforts. In addition, the task force or agency performing the study would not have the benefit of the lessons learned from the establishment of a clearinghouse for best practices in IT security.

The Federal Government Encourages And Supports The Establishment Of A Private Sector Clearinghouse For Best Practices In IT Security

Under this option, NIST would work with private industry to establish a clearinghouse for best practices in IT security within an IT industry association such as ITI or EIA. The private sector industry association serving as the clearinghouse would be expected to maintain and disseminate information concerning these best practices to any public or private organization that requested it. (The fact that ITI formed the Information Security Exploratory Committee (ISEC) at the request of the President is an indication that this option is feasible). However, in order to induce an industry association to accept the larger responsibility of establishing and maintaining a clearinghouse for best practices in IT security, it may be necessary for the government to provide some funding as well as other forms of support.

- **Pro:** This approach would avoid potential competition between government and any private sector organizations considering establishing a clearinghouse for best practices in IT security. It would probably be more cost-effective than establishing a government clearinghouse. A private-sector clearinghouse may be more effective in obtaining information concerning IT security from private sector firms than government. It may tend to establish an infrastructure protection “beachhead” within the private sector that could help government monitor security of IT infrastructure area and encourage development of new IT security products and practices.

- **Con:** This approach ignores a potentially significant need in other infrastructure areas to identify and disseminate best practices in infrastructure security. Private sector industry associations may be unwilling to accept a role as clearinghouse. If the need for IT security is so great, the private sector would likely to establish clearinghouse without a push from government.

Procurement

Establish A Task Force To Determine How Infrastructure Assurance Considerations Might Be Incorporated Into Federal Acquisitions

A task force could review the IT acquisition guidelines to be developed by OMB to determine whether they adequately address infrastructure assurance concerns. To be effective, this option (like a number of the others) requires well-defined infrastructure assurance goals and a clear understanding of what kind of infrastructures, especially within the Federal government, need to be protected and from what kinds of threats.

- **Pro:** This approach appears to be a reasonable first step in attempting to use the procurement process to promote infrastructure assurance. It would help to determine if infrastructure assurance is currently being adequately considered in acquisition programs.

- **Con:** This approach takes a broad perspective across all infrastructure areas where a more specific focus on one or two high risk infrastructure areas, such as telecommunications, may provide faster and more focused results. The government may miss significant opportunities to build-in security within its own infrastructure while it is evaluating the applicability of using procurement to improve infrastructure assurance.

Form A Task Force To Review The Adequacy Of Infrastructure Assurance Provisions In Large Pending Federal Procurements

The focus of this option would be to form a "SWAT" team to ensure that major, near-term Federal acquisitions such as FTS2001 (follow-on to FTS2000) adequately provide for

infrastructure assurance. This option is especially appropriate if current procurement procedures do not adequately consider and provide for infrastructure assurance needs and if a number of specific acquisition programs that should be reviewed can be readily identified.

- **Pro:** This approach involves immediate action to improve assurance of government-owned infrastructures.
- **Con:** The findings are likely to *raise* costs of underlying acquisitions. This approach does nothing to institutionalize infrastructure assurance considerations in Federal acquisition process. Agencies are likely to react negatively to the recommendation to conduct an additional audit of their near-term acquisition programs. Without well-defined assurance goals, this approach might delay or compromise acquisitions without providing significant improvements in infrastructure assurance.

The President Issues An Executive Order Requiring Agencies To Procure Only IT Products And Services That Meet NIST, Commerce, NSA Or Other Agency Security Standards

Under this option, the Federal government would apply the EPA Energy STAR model to IT acquisition. To be viable, this option would require that NIST, Commerce, NSA or another agency establish security standards for IT products and services and develop certification methods for those products and practices that meet the standards.

- **Pro:** This option would promote conformance with established IT security standards throughout the Federal government.
- **Con:** Such a recommendation may be viewed as being premature until the NIST, Commerce or NSA certification process is in place. It might place too much weight on security considerations during IT acquisition process, and would not address other critical infrastructure areas.

Certification Programs

NIST, Commerce, NSA Or Another Agency Works With IT Industry To Evaluate The Advisability And Feasibility Of Certifying Security Protection Of IT Products And Services

Under this option, a Federal agency works with an IT industry association such as the Information Technology Industry Council (ITI) or the Electronics Industry Association (EIA), or forms a joint government/IT industry council, to determine whether IT security could be improved through the certification of IT products and services that meet certain security standards. Among other things, the association group or council would determine the scope of IT products and services to be certified, the feasibility of establishing security standards for these products and services, and define procedures for certifying products and services.

- **Pro:** This approach would enable the government to determine whether the practice of certification is likely to be effective prior to implementation, and would help to define the proper scope of an IT certification program as well as the appropriate role of government. It would also provide early industry reaction to the concept.
- **Con:** It does not address other infrastructure areas besides IT. A recommendation for follow-on study implies more time will pass before specific action is taken, and would delay certification program for IT products and services which may be ready for implementation.

NIST, Commerce, NSA Or Another Agency Works With Industry To Establish Security Standards For IT Products And Services And Develop A Private-Sector Certification Process

The Federal government appears to be already moving toward establishing security standards for IT products and services. Under this option, the Federal government would attempt to accelerate and build on this movement by applying something along the lines of an EPA Energy STAR model to the IT infrastructure area. In addition, some Federal agency or agencies could work

with IT industry groups to establish security standards for IT products and services and develop a process within the private sector for certifying these products and services. Ultimately, an industry association, university center, or FFRDC could assume responsibility for managing the certification process. As in the Energy STAR program, the certifying industry association would provide "SecuritySTAR" labels or a seal to producers to affix to their IT products or service brochures to indicate they are compliant with the IT security standards.

- **Pro:** This approach would increase the market awareness of IT infrastructure security technology by allowing producers of IT products and services to advertise that their products comply with specific industry security standards. The program could involve minimal government expense since industry would administer the largest portions of the certification process. This approach also sets the stage for eventually requiring government agencies to buy only certified IT products and services. Collaboration between government and private sector in setting standards, and private sector management of the certification process would help in gaining industry buy-in for the program.

- **Con:** This approach does not address other infrastructure areas besides IT. An industry association may encounter conflicts of interest in attempting to perform impartial certification of products and services because of its dependence on corporate membership.

NIST, Commerce, NSA Or Another Agency Establishes Security Standards For IT Products And Services, And Certify Those Products And Services That Meet The Standards

This is the same as the earlier option, except that a Federal agency would take full responsibility for establishing IT security standards and performing or contracting for tests to determine if IT products and services meet the security standards.

- **Pro:** This approach would increase market awareness of IT infrastructure security technology, and set the stage for requiring government agencies to buy only certified IT products and services. The public may have more confidence in certification if the tests are performed by the Federal government.

- **Con:** This approach does not address other infrastructure areas besides IT. Private industry may resent and resist a program in which the Federal government establishes standards and performs certification. It is a potentially costly endeavor to certify all current IT products, especially in the constantly-changing IT market, and there may be

a liability issue as well if government-developed standards or government-tested IT products prove faulty.

NIST, Commerce, NSA Or Another Agency Certifies IT Products And Services, And A Follow-On Task Force Is Established To Evaluate The Advisability/Feasibility Of Certifying Assurance Products And Services For Other Infrastructure Areas

This option assumes that the IT certification program will be successful in promoting IT infrastructure assurance.

- **Pro:** This option initiates IT certification program and positions the Federal government to quickly apply practice to other infrastructure areas.
- **Con:** If the IT certification program fails, time and resources invested to study the application of certification to other infrastructure areas will probably have been wasted.

Part Three

Conclusions

The possible permutations of options itemized in the previous section can be reasonably boiled down into the following conclusions as to what would constitute an optimum mix for best ensuring the success of infrastructure assurance initiatives. By virtue of the various competing equities involved, a "blended" approach to various options offers the best combination of political feasibility and the highest probability of achieving infrastructure assurance objectives.

Performance Measurement

The production of a "high risk" report for infrastructure assurance is a laudable goal for a Federal government infrastructure assurance organization. Such a report could make use of information assembled in furtherance of such an organization's responsibility to "assess the national risk." Once sufficient baseline data has been accumulated, the report might take on a more normative character. Furthermore, specifying infrastructure assurance as a strategic goal or category of specific goals under the GPRA or ITMRA frameworks would be very helpful. There appears to be a need for information security considerations to be specifically included in the management framework for information technology acquisition and use as set out in the ITMRA and other pieces of legislation and regulations. There are, however, differences in the respective goals, structure and relative specificity of the GPRA and ITMRA.

Agencies should identify existing infrastructure assurance-related responsibilities and include them in strategic plans submitted in compliance with the GPRA. Agencies should incorporate any new infrastructure assurance-related taskings into strategic plans under the GPRA, thus facilitating coordinated budgetary performance review. Currently, agencies are required by the GPRA to prepare a five year plan including "major functions and operations" of the agency. If an agency does not consider infrastructure assurance to be a "major function or operation," it may not be included in the strategic plan. The failure to include such a function in the five-year plan allows it be left out of the annual performance plan which serves as the foundation for budgetary review. In order to assure performance measures are put in place and reviewed as part of the budget process, infrastructure assurance functions should be explicitly included in agency strategic plans.

- **Pro:** This approach encourages infrastructure assurance to be included in strategic planning, thus facilitating coordinated budget review.

- **Con:** The current rate of implementation of the GPRA has been slow, and this option could promote delay unless used in conjunction with other performance measures.

Congress could also consider the propriety of a modest revision to the ITMRA to encourage agencies to establish security-based performance measures in addition to other performance measures required by the Act (see proposed language in Appendix B).

- **Pro:** This approach promotes agency development of performance measures in a minimally burdensome way, and in a manner likely to lead to the development of government wide standards and best practices.

- **Con:** The effectiveness of implementing ITMRA requirements through agency CIOs remains uncertain.

Publication of Infrastructure Assurance Data

An immediate pilot study ought to be conducted to investigate the feasibility and likely effectiveness of publishing comparative telecommunications or electric utility reliability data in order to accomplish infrastructure assurance objectives.

Publication of performance data (e.g. by the FAA for on-time arrival/departure), is a possible means of increasing general sensitivity to and awareness of reliability, security or other infrastructure-related performance of infrastructure services. In light of deregulation and restructuring of major infrastructures such as telecommunications and electric power, additional information, provided by a neutral source, may allow consumers to make educated choices in selecting between available infrastructure services.

Insofar as publication may be one possible means of promoting infrastructure assurance objectives, the Administration could direct the FCC's Network Reliability and Interoperability Council (NRIC) to initiate a pilot study as to the feasibility of publishing comparative infrastructure assurance-related data for the telecommunications industry.The NRIC could conduct a pilot study of the likely impact and feasibility of such publication.

Such a study that could address, among other issues: (1) the types of infrastructure assurance-related data that could be published; (2) to what degree the practice of publishing infrastructure assurance-related statistics would likely achieve infrastructure assurance objectives; (3) whether effective publication could be accomplished using data already made available to the Federal government, or whether additional data collection might be necessary; and (4) how the practice of publication might influence industry practices, consumer choices, and the liability climate.

- **Pro:** The approach promotes the practice and initiates further study of its application. A careful study will allow complex issues such as liability to be further explored and resolved, and use of a pilot allows the practice to be studied thoroughly before being considered for extension to other infrastructures.
- **Con:** The use a pilot in one industry only may slow the spread of the practice to other areas where it may be needed, particularly by consumers, in the near future.

Identification and Dissemination of Best Practices

Additional research has revealed that under Executive Order 13011, the Government Information Technology Services Board (GITSB) is responsible for collecting and disseminating information on IT best practices for the government. In order to implement this responsibility, GITSB allocated funds to NIST's Computer Security Resource Clearinghouse (CSRC). The CSRC is a website with information available on a wide range of information technology and security issues. The information available originates primarily with NIST, but includes some private sector information of significant impact. The CSRC information is available to both government and private sector. Additional informal avenues are available to government CIOs to share information about IT practices. These include the CIO Council and a GSA inter-agency newsletter on information technology management. Implementation of information security recommendations made by the National Performance Review are still underway.

Existing Federal government efforts to identify and disseminate best practices in information technology could be expanded to promote greater private sector participation and that the resulting efforts be considered as potential models for best practices clearinghouses for other critical infrastructures. Sharing of best practices as mandated by E.O.13011 could be further expanded to draw on the expertise of other government agencies (e.g. NSA) and the private sector. Additional resources should be used to expand awareness and use of the information so collected. It may prove desirable for the CRSC to take a more active role in disseminating information to government IT managers. In concert with the expansion of the CSRC efforts, a study should also be undertaken to determine whether the structure, funding, participants, and

management of the IT best practices effort could be applied to other infrastructure assurance areas. This study could be undertaken by an interagency task force.

- **Pro:** This approach allows the Federal government to highlight best practices as a model performance practice and to endorse the practice in a number of areas while making a specific recommendation for the fortification of current efforts in IT. It also enhances the private sector's role in sharing best practices information with the government while allowing them to benefit through dissemination channels. The option requires only minimal resources to implement and existing channels may be used. Limited success in the IT arena can be achieved before moving to other infrastructure assurance areas.

- **Con:** The current Federal government IT environment has a number of players and can be confusing. This approach does little to simplify the environment.

Procurement

The Administration could identify an interagency task force to (1) identify large pending procurements related to infrastructure assurance issues; (2) study the degree to which large pending procurements adequately address infrastructure assurance objectives, (3) make recommendations as to how such procurements might be adapted, in the short term, without unduly adding to their cost; and (4) based on lessons learned through review of individual procurements, make recommendations as to how the Federal acquisition process might be revised to address infrastructure assurance. The impending re-competition of several long term Federal government contracts (including, for example, FTS 2000) provides an important opportunity for the government to assess the degree to which these contracts reflect infrastructure assurance concerns. An interagency task force should be convened to address the issues raised in those large procurements identified as needing review. The task force could use what is learned from this study to develop recommendations for revising the procurement *process* to better take into account infrastructure assurance objectives (specifically taking into account, for example, the current security criteria in place and the procedures for obtaining waivers). The task force might also consider the feasibility of requiring procurements to meet security standards set out by other government agencies (NIST, NSA, DOE, etc.).

- **Pro:** With such an approach, the Federal government acts quickly to promote infrastructure assurance objectives in large pending procurements, yet allows for informed study of the procurement process using modest resources.

- **Con:** The current procurement environment, marked by the movement to commercially available/off-the-shelf products, may constrain potential recommendations of such a body in all but the truly large-scale procurements.

Certification Programs

Energy STAR is a certification program for energy efficient computer hardware and office equipment administered by the EPA. The Administration could consider programs like the EnergySTAR certification program as a potential model to guide infrastructure assurance efforts.

Energy STAR is enforced by Memoranda of Understanding between the company seeking to use the logo and the EPA. The MOUs dictate the appropriate uses of the Energy STAR logo and allow companies to self-test or employ a third party to test the products for compliance with the EPA standards. EPA spot checks products for compliance with standards and to ensure that only companies with an MOU are using the logo. In the event a company is not in compliance, EPA will generally attempt to resolve the issue informally. If that fails, EPA will require that the company either meet the standards or remove the label.

The Energy STAR program could provide an effective model for government programs aimed at the certification of IT products and services. Consideration of such a program might also encourage development of similar programs in other infrastructure areas to promote assurance objectives. The Energy STAR program may be held up as an efficient and appropriate use of government authority and resources, and advocates its broad consideration as a potential model for other government programs aimed at promoting infrastructure assurance through government and private sector adoption and implementation of certification standards.

- **Pro:** This approach would highlight the success of the Federal government initiative while providing a useful model for a certification process. It carries the additional benefit of low costs of implementation and enforcement and high visibility.

- **Con:** Merely acknowledging the effectiveness or appropriateness of a model does not, in itself, significantly further the effort.

Standards

Before meaningful certification programs can be established, standards must be in place to guide the certification process. There are many means by which the government can develop standards, however, in advocating a performance-based approach to certification, and a similar approach can be taken with regard to standards development as well. Research was performed into the various mechanisms by which the Federal government can influence or engage in the standards development process. The results of that research are attached as a supplemental report. (S*ee* Appendix C.)

Appendix A

Summary of Procurement Trends and Legislation[1]

Background

The Department of Defense (DoD) is the world's largest buyer of goods and services. In Fiscal Year 1996, DoD completed over 8.7 million procurement actions, of which more than 8.4 million were for purchases under $25,000. These purchasing actions involved the efforts of more than 20,000 contracting personnel in over 1,300 contracting offices worldwide. Virtually all procurement actions under $100,000 require significant time and effort to define needs, identify funding, define sources and secure contracts. The acquisition reforms recently enacted are intended to streamline the acquisition process for goods and services valued under $100,000.

Two major reforms in DoD acquisitions were the increase of the small purchase threshold from $25,000 to $100,000 and the institution of the International Merchants Purchase Authorization Card (IMPAC). By increasing the small purchase threshold to $100,000, DoD contracting officers are not required to issue notices in the Commerce Business Daily (CBD) and may solicit from a short list of vendors. With the IMPAC card, buyers holding the card may purchase goods and services in the same way as a customer holding a VISA credit card, reducing the amount of paperwork and time required by DoD buyers.

[1] This appendix was prepared by Mr. Paul Harder of SRA International.

Regulatory Reform

The last three years have witnessed radical reforms in government procurement regulations. Three key reform acts have resulted in a vastly different landscape for government buyers. Below are the three Federal acts, with a summary of the changes which affect acquisitions under $100,000.

Federal Acquisition Streamlining Act of 1994 (FASA)

The Federal Acquisition Streamlining Act of 1994 (FASA) (Public Law 101-365) made a number of changes in the way goods and services at, or below, $100,000 are acquired. The Act replaces the $25,000 threshold with a new "Simplified Acquisition Threshold" (SAT) of $100,000 once an agency (or procuring activity within the agency) has achieved certain electronic commerce (FACNET) capabilities, is using them and certifies that they have met the criteria. Until that time, the threshold is only increased to $50,000.

Other key changes made to procurement of goods and services below $100,000 are:

- Quotes will be solicited in writing 15 days after placing a notice in the Commerce Business Daily (CBD). The notice may be used: (1) to ask for expressions of interest from vendors so that after the 15-day waiting period they may be requested, in writing, to submit a quotation, or (2) to request written quotations, to be submitted within a reasonable time after the 15-day waiting period. In addition, the CBD notice will contain: (1) an accurate description of the product(s) to be acquired, (2) a description of the procedures to be used to select and make the award, (3) a statement reserving the procurement for small business, and (4) a statement of the period of time expected for the contracting officer to solicit/evaluate vendor quotes, and issue the purchase order. All quotes received from a small business will be considered.

- FASA reserves new contracts, above $2,500 but under the simplified acquisition threshold, for small business. It specifically authorizes continued set-asides of all contracts under the threshold for minority small businesses. However, FASA excludes purchases of $2,500 or less (Micro-Purchases) from the small business reservation, to make it possible for agency officials to make simplified purchases and credit card purchases. These purchases do not have to be competitive and are exempt from the Buy American Act.

- FASA eliminated the applicability of several FAR solicitation clauses to SAT transactions and established a $100,000 threshold for fifteen (15) different statutes that establish paperwork and recordkeeping requirements not applicable in the commercial sector.

FASA retains the requirement that a notice of any procurement over $25,000 be published in the Commerce Business Daily 15 days prior to the issuance of a solicitation. After the issuance of this notice, however, simplified acquisitions could follow any procedures described in the notice -- for example, by shortening the period for submission of offers.

FASA phases out the requirement to publish advance notice of purchases below $100,000 when electronic commerce procedures and systems (interim FACNET) are in place. It also provides that all procurements of $250,000 or less need not be synopsized in the CBD if a "full FACNET" system is being used for the procurement.

Federal Acquisition Reform Act of 1995 (FARA)

FARA revises the standard for "full and open competition" for procurement of goods and services to provide for open access to bidding that is "consistent with the need to efficiently fulfill the Government's requirements." The Act also revises requirements for the use of other than competitive procedures, allowing such procedures only when the use of competitive procedures is not feasible or appropriate. Standards for making this determination are to be set forth in the Federal Acquisition Regulation (FAR).

FARA provides that the FAR shall ensure that the requirement to obtain full and open competition is implemented in a manner that is consistent with the need to fulfill the Government's requirements efficiently. However, this provision makes no change to the requirement for full and open competition, nor to the definition of full and open competition. Therefore, it is unclear how this requirement will be implemented.

FARA prohibits sole source procurements of commercial items valued above the simplified acquisition threshold "unless the need to do so is justified in writing and approved in accordance with the [FAR]." Section 4202 of FARA permits the use of simplified acquisition procedures for procurements expected to exceed the simplified acquisition threshold, but not to exceed $5 million, when the contracting officer reasonably expects, based on the nature of the property or services and market research, that offers will include only commercial items.

Regarding Commercial-Off-The-Shelf (COTS) products, FARA provides that the FAR shall include a list of provisions that are inapplicable to contracts for the procurement of commercially available off-the-shelf items. The House-Senate Conference Report states that the list would include each provision of law that, in the opinion of the Administrator of the Office of Federal Procurement Policy (OFPP), imposes government-unique policies, procedures, requirements, or

restrictions, except any which the Administrator determines it would be in the best interests of the United States to include in contracts for commercially available off-the-shelf items. The list would not include generally applicable provisions of law (i.e., those not uniquely applicable to government contractors) nor several categories of statutes, such as any that provide for civil or criminal penalties.

FARA also expanded the definition of "commercial services" to include services sold based on "market" as well as catalog prices. The new definition reads: "Services offered and sold competitively, in substantial quantities, in the commercial marketplace based on established catalog [or market] prices for the specific tasks performed and under standard commercial terms and conditions." This revision allows service firms to qualify as commercial services by charging market prices, which are defined as prices that are established in the ordinary course of trade between buyers and sellers free to bargain and that can be substantiated from sources independent of the offeror.

Finally, FARA amends FASA by eliminating the $50,000 cap on use of simplified acquisition procedures until an agency receives interim FACNET certification (i.e., all activities may use simplified acquisition procedures for procurements up to $100,000). Further, it provides that the threshold will revert back to $50,000 after 31 DEC 1999 if an agency does not have full FACNET certification.

The Information Technology Management Reform Act of 1996 (Section E of the FY96 Defense Authorization Act) also known as the Clinger-Cohen Act

The Information Technology Management Reform Act of 1996 (ITMRA), radically changes the way information technology (IT) goods and services are procured within the Federal Government. ITMRA repeals the Brooks Act, thereby eliminating GSA's role in the oversight of IT acquisitions and the requirement for agencies to get a Delegation of Procurement Authority (DPA) from GSA.

Agencies are given the direct authority to procure IT with a focus on capital planning and investment control and performance and results-based management. Agencies are required to designate a Chief Information Officer (Section 5125). OMB is given an enhanced role in IT management and oversight including evaluations of agency IT programs and investments. National security systems are exempted from some of the Act's requirements.

Procedures required for IT acquisitions are destined to change due to a requirement that the FAR Council ensure that the process for acquisition of IT is simplified, clear, and understandable and specifically addresses the management of risk, incremental acquisitions, and the need to incorporate commercial IT in a timely manner. Also, ITMRA directs agency heads to use

"modular contracting" to the maximum extent practicable for the acquisition of major IT systems. The Act describes modular contracting as an approach under which an "agency's need for a system is satisfied in successive acquisitions of interoperable increments. Each increment complies with common or commercially accepted standards...so the increments are compatible with other increments...comprising the system." The FAR must provide that a contract for an increment of an IT system should be awarded within 180 days after the solicitation is issued, and if it cannot be, the increment should be considered for cancellation.

The critical portion of ITMRA with respect to small purchases is the requirement that by January 1, 1998, FACNET (or, if use of FACNET is not practical, another automated system) must provide government-wide on-line computer access to information on products and services that are available for ordering under the GSA multiple award schedules. This is precisely the requirement which will be addressed herein.

Significant Policy Changes

The past three years have also resulted in significant changes in the policies surrounding defense acquisitions. This change reflects the Defense Department's interest in becoming less of a driver of technology, specifying what goods and services should look like and becoming more of a buyer of technology, looking for the best commercially available unit to meet the government's requirements.

The Defense Department's change is reflected in their approach to specifications. During the past three years, DoD has eliminated over one hundred military specifications and standards, replacing them with equivalent commercial specifications and standards. By doing this, DoD opens the doors to new commercial vendors to provide goods to meet the needs of the warfighter without having to re-tool or re-manufacture goods to meet a specific military requirement. Instead, the same product which meets the commercial market's standards may also meet the military's standards.

Another change is the renewed emphasis on using existing contracts rather than entering into new contracts. DoD has ordered its personnel to maximize use of the GSA schedules for goods and services and to minimize the use of new contracts where possible. This shift away from making contracts whenever a need arose to consulting a pre-negotiated contract before starting a new contract is a shift in the procurement mindset.

Further enabling this shift has been the creation of electronic catalogs. Through the Internet, government buyers have been able to procure goods and services through electronic catalogs like GSAdvantage! and the DLA Buyer website. Further, Dr. Steve Kelman, Administrator of the Office of Federal Procurement Policy issued on March 14, 1997 a policy statement on Electronic

Catalogs. “Electronic Catalogs” are defined by OFPP as a Web-based electronic ordering system which involves: (1) a contract with pre-established business arrangements with industry; (2) a means for the customer to identify and order goods and services, either from within an agency (intra-agency) or by more than one agency (inter-agency); and (3) sufficient information (updated to reflect changes) for the customer to compare the items offered by performance, price and delivery.

Dr. Kelman recognized that electronic catalogs were the way of the future for federal acquisitions. He stated that:

> “Electronic catalogs have become a prime method for us to take advantage of the operational efficiencies offered by evolving electronic commerce technologies. I encourage you, in your efforts to provide greater value to the taxpayer, to aggressively promote the use of Federal electronic catalogs. As our use of this evolving technology increases, however, there is a corresponding need for greater interagency coordination to maximize the effective use of electronic catalogs.”

Electronic catalogs offer two advantages. They require fewer resources to make repetitive purchases and they offer opportunities for agencies to pursue more effective purchasing strategies. They can help the federal government leverage its buying power through volume purchasing. Alternatively, they enable government customers to make "spot" purchases with on-line comparisons of the price, features, and performance of similar products and services.

Appendix B

Information Technology Management Reform Act

Proposed revisions as marked

Sec. 5123 Performance and Results-Based Management

In fulfilling the responsibilities under section 3506(h) of title 44, United States Code, the head of an executive agency shall--

(1) establish goals for improving the efficiency ~~and~~ effectiveness**, and security** of agency operations and, as appropriate, the delivery of services to the public through the effective use of information technology;

(2) prepare an annual report, to be included in the executive agency's budget submission to Congress, on the progress in achieving the goals;

(3) ensure that performance measurements are prescribed for information technology used by or to be acquired for, the executive agency and that the performance measurements measure **the level of security of the information technology, and** how well the information technology supports programs of the executive agency;...

* * *

(4) ensure that the information security policies, procedures, and practices of the executive agency are adequate.

Appendix C

Federal Role In Development Of Standards[1]

This discussion examines ways the Federal government can provide incentives and promote the standards settings process without necessarily requiring or mandating the setting or use of such standards. The Legal Team conducted research on available methods for creating such incentives. These efforts have been fruitful and may merit further consideration.

Background

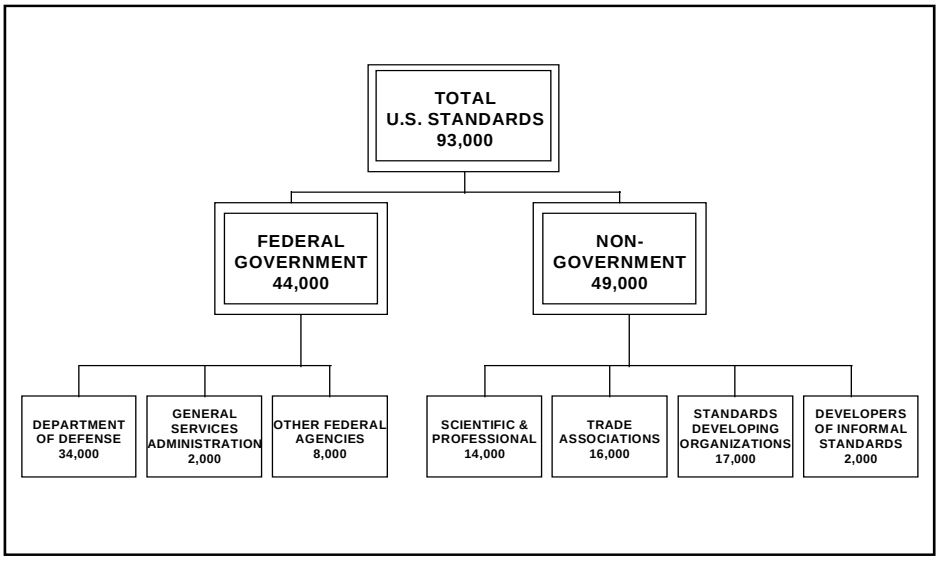
The U.S. standardization system is quite complex compared to those of other countries. In the United States alone, there are 700 organizations that take part in the standardization process. Both government and non-government organizations have an almost equal hand in the system. Of the 93,000 standards in the United States, the Federal government developed 44,000 and non-government organizations developed 49,000. Major players include Federal government agencies, scientific and professional organizations, trade associations, standards developing organizations, and developers of informal standards.

The leading standards developers in the government include the Department of Defense (DoD) and the General Services Administration. Although 80 government organizations have developed standards, these two organizations alone account for over 80 percent of Federally developed standards and almost 40 percent of all U.S. developed standards. Most government standards are developed for either internal or regulatory use, although there are a few cases where the government coordinates the development of voluntary standards for the private sector.

[1] This appendix was prepared by Elizabeth A. Banker, Assistant General Counsel to the President's Commission on Critical Infrastructure Protection (PCCIP). Background research was compiled by Mr. Ted Drake of SRA International.

In the private sector, over 620 organizations take part in the standards development process. The American National Standards Institute (ANSI) coordinates 175 of these organizations, promoting the development of voluntary, consensus-developed standards. Other large non-government standards developers include the American Society for Testing and Materials, the U.S. Pharmacopeial Convention, the Society of Automotive Engineers International, and the Aerospace Industries Association.

Figure 1. Number of U.S. Standards by Type of Organization



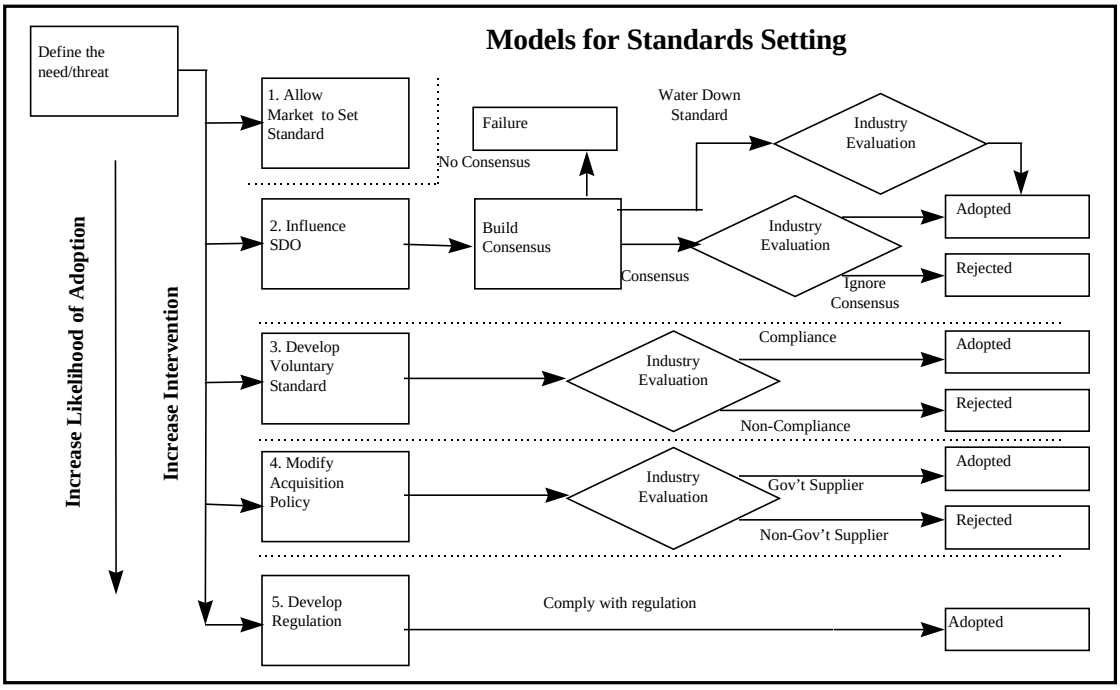
The following sections will discuss the standards development process from a government perspective, focusing on methods that the government can use to facilitate standards development. We will look at industry evaluation and adoption of standards and obstacles to the development of effective standards. We will discuss relevant legislation as well as the government's role in the standards development process.

Models for Standards Setting

Figure 2. provides a framework for analyzing the standards development process from a government perspective. The Federal government has several options, involving varying degrees of intervention, for developing a standard. Once the government has defined a need for a

standard, it has five options ranging from letting the market develop the standard to specifying compliance with a standard in government regulation. Figure 2. illustrates these options and the associated outcomes of each. As the government increases its intervention in the standardization process, it also increases the likelihood that the industry will adopt the proposed standards. However, with more intervention, there are additional costs that will be placed on the affected industry, and the longer it will take.

Figure 2. Models for Standards Setting



Allow The Market To Set Standards

In many cases, the market will develop and implement standards on its own. There are two key players in this area, standards developers and standards development coordinators. Developers include industry organizations, professional associations, and standards development organizations. Coordination programs facilitate both the development of "needs" for standards, as well as the actual development and implementation of standards among the various standards developers.

ANSI is the leader in the coordination and facilitation of standards within the private sector. Founded in 1918 by five engineering societies and three government agencies, ANSI remains a private non-profit organization. The organization's goal is to enhance the global competitiveness

of U.S. business and the American quality of life by promoting and facilitating voluntary consensus standards. ANSI accredits 175 standards developing organizations that follow specific procedures regarding the development of standards. In addition, it reviews standards that are submitted by accredited organizations. If the standards satisfy certain requirements, they are labeled as American National Standards. The Information Infrastructure Standards Panel (IISP), a high-level arm of ANSI, promotes and accelerates the cross-industry coordination of national and global standards for the deployment of the information infrastructure. The panel tries to identify and obtain sponsors for needed standards.

Influence Standards Developing Organizations

There is significant opportunity for the Federal government to influence private sector standards development. Most standards development organizations are completely open to external involvement. ANSI, in particular, has many government members participating on its boards and committees. Both NIST and DoD actually track employee participation in these committees, and manage this participation to ensure that there are no "holes" in coverage.

The National Institute for Standards and Technology (NIST) plays the role as the Federal government's chief coordinator for the development and maintenance of standards. The Interagency Committee on Standards Policy (ICSP), within NIST, brings together representatives from each Federal executive agency to promote effective and consistent standards policies in furtherance of U.S. domestic and foreign goals. NIST has over three hundred employees who participate on the technical committees of various standards developing organizations. In many cases, NIST works directly with these organizations to develop standards requested by government agencies.

The Department of Defense (DoD), as the largest standards developer in the United States, develops its own requirements as well as works with other standards organizations to develop new standards. DoD participates as an "equal partner" with the private sector and other government agencies on the technical committees of non-government standards bodies. The Department's goal is to ensure the proper consideration of DoD requirements, enhance the technical knowledge of DoD personnel, and allow the DoD to contribute its considerable technical capacity. The Department of Defense monitors its influence through the SD-11 database, which identifies and tracks the many DoD personnel who participate on these technical committees. This allows the Department to manage its resources by determining where participation is adequate, and where it is weak and requires increased support.

This option is of particular interest because all standards are developed through a consensus process, which requires the involvement of all interests including the government. This adds significant weight to the standard when it goes to the evaluation and adoption process. Since all interests are involved, it is much more likely that the standard will be adopted by the affected industry and adhered to in the long run.

Develop Voluntary Standards

In some cases, the Federal government has actually developed voluntary standards for use in the private sector. This usually occurs in markets or industries where private sector organizations have failed to provide sufficient coverage with regard to standards development. The government has assisted in the development of standards where liability issues have kept other private organizations away. For example, NIST coordinates the development and maintenance of voluntary product standards for softwood lumber and construction. Private organizations have shied away from developing standards in these two areas because of various liability issues.

In addition to the direct development of voluntary standards, the government can offer incentives to organizations to develop standards in a particular area. In the past, these incentives have been in the form of grants and subsidies. For example, pursuant to the Goals 2000: Educate America Act, 20 U.S.C. § 5932 *et seq*., the Federal government established the National Skills Standards Board (NSSB). Even though Congress created the NSSB, it is not a government agency. It is a group of business, education, labor and civic leaders dedicated to encouraging the development of voluntary skill standards.

To accomplish its goal, the NSSB "awards grants to voluntary partnerships for the development of [the] skill standards." 20 U.S.C. § 5934(g). The NSSB determines the career fields where skill standards are needed and then accepts proposals from interested groups to set the necessary standards. Funds are awarded to associations or coalitions that demonstrate an ability to convene key stakeholders in specific industry sectors in order to set the necessary standards. The NSSB then approves the standards proposed by the grantees.

The Goals 2000: Educate America Act was passed after 10 years of looking at what was wrong with the United States education system. Some believed that our education system was in a perilous condition and that the Federal government had not done enough to improve it. (cite Mr. Biden & Mr. Chafee, Senate 2/8/94) Presently, the NSSB is thought to be an organization that is trying to keep ahead of a rapidly changing environment.

Modify Acquisition Policy

Many agencies use acquisition policy as a way to influence standards development. This is particularly effective when the government has a large market share for the product being supplied. Acquisition policies result in supplier compliance, but may also have an effect on non-suppliers who are interested in supplying products to the government. On the downside, in those areas where the government has a minimal market share, acquisition policies may not have any effect outside of the government.

Develop Regulation

Developing and instituting a regulation is always an option, but there is a significant downside. Lack of involvement of the private sector in the development process may result in lackluster adherence to the regulation. In addition, regulations may place significant costs on the affected industries. In the area of information technology, where conditions change rapidly, regulation would be hard pressed to keep up and remain appropriate.

Industry Evaluation

The most important step in the voluntary standards development process is to obtain industry approval for the proposed standard. This applies to every standards development model, with the exception of government regulations. There are several factors that increase the likelihood that a standard will be accepted. Clearly, the more benefits that accrue from a standard, the more likely it is to be adopted. Standards that promote compatibility, efficiency, and reliability are much more likely to be implemented by industry. A standard that increases the market share of a particular industry sector or serves to reduce an industry's liability in a particular area tend to be more successful as well.

Product standards are more likely to be accepted when the "users" of the product have a hand in the standard's development rather than the suppliers or producers. When suppliers are involved in the development process, they tend to advocate much more generic standards so as not to make any particular supplier's product obsolete. Users, when involved in the process, develop more specific standards especially with regard to reliability and compatibility.

The aerospace industry is a good example. A typical aircraft, whether military or commercial, contains an extensive array of parts and components. An exceptional number of these parts (60 to 70 percent) are defined by standards developed by the aerospace industry. Aerospace customers are very interested in parts reliability and compatibility among different types of planes, and, in part, drive the development of many of these standards.

In addition, the "users" of these parts (airplane manufacturers) are extensively involved in the development of aerospace standards, and promote the development of well-defined aviation standards. As a result, the industry has a significant number of distinct standards for airplane parts.

In comparison, the automobile industry is much less organized in the standards arena. Suppliers have a much greater role in standards development, while automobile consumers have little role. This results in a situation opposite to that of the aerospace industry. The industry uses a much

smaller number of standardized parts, and the standards that they do have are much more generic. This is evidenced by the multitudes of proprietary parts that currently exist in the automobile industry today.

Obstacles Which Prevent the Efficient Development of Standards

Several obstacles exist that can prevent standards from being established relatively efficiently by the public and private sectors. Organizational issues can distort the process. These include decentralization, market incentives, and antitrust issues.

The decentralization of the U.S. voluntary standardization system is one of these obstacles. Compared with other countries, the United States has no central authority for standards development. The American National Standards Institute (ANSI) is the primary coordinator in the private sector, but it only has a minor hold on the standards market. In total, there are over 600 private sector organizations involved in standards development. Approximately 175 of these organizations are ANSI accredited. While ANSI accredited organizations account for over 75 percent (36,000) of non-government standards, only a third (11,500) of these standards are actually certified as American National Standards. There are so many organizations involved in standards development that it makes it difficult to coordinate the development of a standard. Competing organizations often develop different standards for similar products. In the building and construction sector, there are more than 12,000 standards alone. This creates the problem of deciding which standards to implement in an organization.

Compared to the United States, Canada has a much more centralized system for developing standards. The primary standards body is the Standards Council of Canada, a body of the Canadian government. The Standards Council of Canada is a federal Crown Corporation with the mandate to foster and promote voluntary standardization for the benefit of industry, consumers, and the economy. The council has the legal mandate to accredit organizations performing standards development functions. As a result of this coordination, Canada has significantly fewer standards and standards developing organizations than the United States.

Market incentives may hinder the efficient development of standards. In the private sector, the development of standards is supply-driven. Most standards development organizations fund their operations through membership fees and the sale of standards, creating an incentive to develop standards for income rather than need. As a result, a relative glut of standards has emerged and the quality and specificity of these standards has decreased. The United States has three times the number of standards as Germany, the second largest standards developer in the world. In addition, many of these standards are unused because they are either obsolete or too generic for

their purpose. It is estimated that 25 to 30 percent of our national standards, both government and industry, apply to obsolete technology. Often, standards are redundant or overlap one another.

Antitrust issues may hinder the full consideration of certain issues in the private sector. Industry organizations and standards development organizations must be particularly careful in working within the antitrust regulations in the development of product standards. Most organizations have strict guidelines as to what participants may or may not discuss in the course of deliberations. In some cases, this may prevent the complete consideration of certain standards.

Relevant Legislation/Government Role

There are two recent pieces of legislation that have served to modify the Federal government's role in the standards arena. OMB Circular A-119 set policy regarding the government's procurement and regulatory activities. The Circular states that the government should rely on voluntary standards, both domestic and international, wherever feasible and consistent with the law. In addition, it requested that government agencies participate in and coordinate their participation in voluntary standards bodies. As a result of this legislation, many Federal agencies have started to adopt voluntary standards and include them in regulatory actions. The DoD and NIST have a significant number of employees now participating in standards development organizations. As noted above, agencies like DoD are starting to track their participation to manage their influence in these organizations.

The National Technology Transfer and Advancement Act sets several requirements for NIST. The Act requires NIST to compare standards used in the private sector with standards adopted by the Federal government and coordinate the use of private sector standards by Federal agencies. NIST is to coordinate public and private standards activities to eliminate unnecessary duplication and complexity. This act basically gives NIST the role of standards coordinator for the Federal government. NIST has the mandate to be the primary facilitator of standards in the United States. In response to this, NIST has increased its influence in various standards development organizations, but has much work to do to integrate public and private standards development.

Analysis

Standards may currently be lacking in important areas of the critical infrastructures. Normally, the market will respond to such a void and fill it through the numerous private standards organizations working today within the United States. In some cases, the market may not identify the same needs for standards as does the Federal government. It may be appropriate for the Federal government to take action to fill that void. Five options to fill the void have been identified. However, only two of those options are truly consistent with an overall approach favoring market forces to work with only minimal coaxing through incentives and other indirect means.

Given recent legislation and the value of consensus, the most appropriate way for the Federal government to promote standards is to allow relevant markets to set the standards, and to help standards-developing organizations identify needed standards and incentivize the process. Both OMB Circular A-119 and the Federal Technology Transfer and Advancement Act have shifted the government's focus from the development of required government standards to the use of non-government voluntary standards. It is also important to understand the market factors that influence the evolution and adoption of standards. Industry organization and the costs/benefits of a standard can drive or inhibit industry adoption of a standard. The Federal government has several opportunities to influence the standards development system, but must clearly define the need for a standard as well as address any market factors that could influence industry acceptance.

The NSSB is one example of such an approach to standards. The Federal government, through the Congress, responded to an apparent void in the education and training leading to the job market because of undefined skill requirements for positions which should be uniform throughout the country. The mechanism the Congress designed allows private sector representatives which wholly comprise and run the NSSB to identify where the voids are and to chose those most capable of creating the standards to fill the void. The only role for the Federal government is one of funding.

The Federal government could also fund efforts of existing standard setting bodies to pursue specific projects. For example, through NIST or another agency, the government could sponsor a group like ANSI's standard setting process in a specific area where the Federal agency felt there was a void. This type of approach allows the government more control over the direction of the process, however, because of Federal involvement in many of the standard setting bodies' work and the Federal allocation of funds, private sector groups may be reluctant to participate because of the degree of Federal control.

The best way to take advantage of the numerous benefits of private standard setting processes it likely a combination of the two approaches.

Conclusion

The Administration should consider putting forth recommendations in the standards area for the following purposes: (1) promoting standards setting in areas where the market is not sufficient to spur development of private sector standards; (2) alleviating the burden on already taxed Federal bodies with standard setting responsibilities; and (3) providing additional support for existing Federal standards bodies.

In order to further these ends, the following steps should be considered:

- The Federal government should find ways to use Federal funds and other incentives to promote creation of standards, by the private sector or by government, in productive areas where the market alone has not yet prompted the need for such standards (including the development of government standards).

- Congress should consider the creation of a government-funded private sector board, modeled on the NSSB, to identify areas where standards are needed and to make grants available to deserving standard setting bodies for projects related to infrastructure assurance objectives, including information technology.